Duty Statement

Classification: **Career Executive Assignment**

Position Number: **275-817-7500-001** HCM#: **5467**

Branch/Section: **Information Technology Services Branch / Information Security Office**

Location: **Sacramento, CA** Effective Date: **January 19th, 2019**

Working Title: **Chief Information Security Officer**

Collective Bargaining Identifier (CBID): **M01** Supervision Exercised: ☒ **Yes** ☐ **No**

Under the general direction of the General Counsel, the Chief Information Security Officer (CISO) provides direction and policy guidance to the Information Security Office, the Information Technology Services Branch (ITSB), and the CalPERS enterprise. The CISO provides direction on information security and privacy across all of CalPERS retirement, health, and investment programs. This position has broad authority and management responsibility for protecting the privacy, confidentiality, integrity, and availability of CalPERS information and services. The CISO aligns services responsible for information security, privacy, and security operations to enable CalPERS business objectives within acceptable levels of security and privacy risk. The CISO will work primarily in the Information Security Engineering domain.

The CISO works closely with the ITSB. The ITSB provides the technology solutions and services that support the CalPERS lines of business. The ITSB includes technology infrastructure, operations, enterprise solutions, and security. ITSB's mission is to add business value by delivering high-quality services, developing partnerships, and contributing to business efficiencies while optimizing the staff/employer/member experience. ITSB is committed to providing the technical leadership, business alignment, talent, transparency, and accountability to support CalPERS strategic business objectives.

Essential Functions

40% Responsible for administering a strategic, comprehensive information security and privacy program to ensure appropriate levels of confidentiality, integrity, availability, and privacy of information assets owned, controlled and/or processed by CalPERS. Plans and executes the enterprise information security and privacy policy, strategy, and best practices. Collaborates with business and IT leaders to maintain security and privacy standards and action plans. Ensures alignment of the information security vision and strategy to organizational priorities to enable and facilitate business objectives, and ensure senior stakeholder buy-in and mandate. Works effectively with business units to facilitate information security risk assessment and risk management processes. Creates a risk-based process for the assessment and mitigation of any information security risk in the ecosystem consisting of supply chain partners, vendors, consumers and any other third parties. Defines and facilitates the processes for information security risk and for legal and regulatory assessments, including the reporting and oversight of treatment efforts to address negative findings. Oversees information and technology dependencies outside of direct organizational control; including the review of contracts and the creation of alternatives for managing risk. Manages and contains information security incidents and events to protect corporate IT assets, intellectual property, regulated data and the company's reputation. Monitors the external threat environment for emerging threats and advises relevant stakeholders on the appropriate courses of action.

Responsible for hiring/assists in hiring, developing and retaining a competent and professional staff that assures an adequate level of specialized analytical and technical expertise to support current and future CalPERS' needs; responsible for outlining performance expectations. Communicates ITSB, Division, team priorities and objectives to staff and facilitates feedback from staff. Ensures organizational policies and procedures are followed. Establishes work assignments, provides direction, and evaluates work quality and customer satisfaction. Creates and maintains a working environment that fosters skill development in staff, discovers and utilizes training opportunities, and provides developmental or corrective training as required. Ensures that an analytical and technical training program is developed, maintained, and executed. Monitors progress on assignments and takes appropriate action to ensure timely and successful completion. Motivates staff to achieve and sustain high performance; establishes and maintains proper staff recognition mechanisms.

25% Administers the information security and privacy governance structure through the hierarchical governance program, including the Information Security Steering Committee. Provides regular reporting on the status of the information security program, and emerging risks, to enterprise risk teams, senior business leaders and the Board of Administration as part of a strategic enterprise risk management program. Manages an information security awareness training program for all employees, contractors and approved system users, and establishes metrics to measure the effectiveness of this security training program. Understands and interacts with related disciplines through committees to ensure the consistent application of policies and standards across all business and technology projects, systems and services; including privacy, risk management, and compliance.

20% Oversees and provides policy direction for the CalPERS privacy program that balances privacy and business usage for CalPERS member, business partner, and stakeholder information. Improves the use of the data to drive security and protection to CalPERS, its members, employees and third-party associates. Ensures that all information owned, collected or controlled by or on behalf of the company is processed and stored in accordance with applicable laws and other global regulatory requirements, such as data privacy.

15% Acts as an advocate for information security and privacy best practices. Consults with senior IT and business leaders regarding their information security risks and responsibility in minimizing those risks. Must maintain reliable, up-to-date, information from the government and across the industry regarding identification of new threats and vulnerabilities. Creates the necessary internal networks among the information security team and line-of-business executives, corporate compliance, audit, physical security, legal and HR management teams to ensure alignment. Maintains external networks consisting of industry peers, ecosystem partners, vendors and other relevant parties to address common trends, findings, incidents and cybersecurity risks. Liaises with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organization maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies. Liaise with the Information Technology teams to build alignment between the security, architecture, infrastructure and application development, thus ensuring that information security requirements are implicit in these architectures and security is built in by design.

Knowledge, Skills, and Abilities

Applicants must possess the ability to perform high administrative and policy-influencing functions effectively. Such overall ability is demonstrated by the following more specific knowledge and ability requirements:

Knowledge of the organization and functions of California State Government including the organization and practices of the Legislature and the Executive Branch; principles, practices, and trends of public administration, organization, and management; techniques of organizing and motivating groups; program development and evaluation; methods of administrative problem solving; principles and practices of policy formulation and development; personnel management techniques; the department's or agency's equal employment opportunity objectives; and a manager's role in the equal employment opportunity program.

Ability to plan, organize, and direct the work of multidisciplinary professional and administrative staff; analyze administrative policies, organization, procedures, and practices; integrate the activities of a diverse program to attain common goals; gain the confidence and support of top level administrators and advise them on a wide range of administrative matters; develop cooperative working relationships with representatives of all levels of government, the public, and the Legislative and Executive Branches; analyze complex problems and recommend effective courses of action; prepare and review reports; and effectively contribute to the department's or agency's equal employment opportunity objectives.

These knowledge and abilities are expected to be obtained from the following kinds of experience (experience may have been paid or volunteer; in State service, other government settings, or in a private organization):

Desirable Qualifications

- Minimum of seven to 10 years of experience in a combination of risk management, information security, and IT jobs (at least five must be in a senior leadership role)
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate information security and risk-related concepts to technical and nontechnical audiences at various hierarchical levels, ranging from board members to technical specialists
- Knowledge and understanding of relevant legal and regulatory requirements, such as: Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry/Data Security Standard.
- Project management skills: financial/budget management, scheduling and resource management
- Knowledge of common information security management frameworks, such as International Standard Organization/International Electrotechnical Commission (ISO/IEC) 27001, Control Objective for Information and Related Technology (COBIT) as well as those from The National Institute of Standards and Technology (NIST), including 800-53 and Cybersecurity Framework
- Professional security management certification is desirable, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.
- Excellent communication, interpersonal relationship management, time management, research/information-gathering skills with the proven ability to work with all levels of an organization
- Ability to exhibit strong leadership and team building skills
- Ability to facilitate meetings with stakeholders
- Ability to present to a wide variety of audiences
- Ability to describe complex technical concepts in terms business leaders can understand
- Ability to maintain effectiveness in varying responsibilities and changing priorities
- Experience with establishing policies and standards, process improvement, etc.

Conduct, Attendance and Performance Expectations

- Ability to maintain consistent attendance
- Ability to demonstrate punctuality, initiative, and dependability
- Ability to model and support CalPERS Core Values (Integrity, Accountability, Respect, Openness, Quality and Balance)
- Ability to model CalPERS Competencies and demonstrate proficiency in; Collaboration, Leading People, Leading Change, Driving Results, Business Acumen, Communication, and Leading Self.

I have read and understood the duties and essential functions of the position and can perform these duties with or without reasonable accommodation.

Employee Name:

Employee Signature: ____________________________________ **Date**:

I certify that the above accurately represent the duties of the position.

Supervisor Signature: ____________________________________ **Date**: